IT3070
Information Assurance & Security
3rd Year 1st Semester

Assignment 1
2024

IAS Risk Management Assignment

Submitted to

Sri Lanka Institute of Information Technology
In partial fulfillment of the requirements for the
Bachelor of Science Special Honors Degree in Information Technology

19.09.2024

Cargills

Submitted by:

Selected Asset	Name	IT Number
Supply Chain Management System	W.A.O.H.Wanasekara	IT22170934
Payroll & Protected Data	T.E.M.D.H.Ekanayake	IT22187550
Retail Point-of-Sale (POS) System	W.K.V Bhashitha	IT22186256

Leader Group Batch & Lab Group : Y3.S1.WE.IT.0202

Table Of Content

1. Introduction

Cargills Ceylon PLC is more than just a retail giant it is a Sri Lankan institution that connects consumers with fresh produce and everyday essentials. Founded in 1844, Cargills has grown from a single outlet into a trusted name in the Sri Lankan retail industry, known for its commitment to quality, sustainability, and community welfare. Through its vast network of supermarkets, food processing units, and restaurants, Cargills seamlessly bridges the gap between local farmers and urban consumers, creating a reliable supply chain that serves millions across the island.

At the heart of Cargills is a mission to uplift local agriculture, ensuring that Sri Lankan farmers are empowered through fair prices and sustainable practices. This ethos of community building has allowed Cargills to evolve from a retail business into a comprehensive platform that supports local livelihoods while delivering fresh, quality products to customers. Whether it's through its supermarkets, dairy production, or processed foods, Cargills is constantly innovating to ensure accessibility and quality for all Sri Lankans.

Cargills dedication to food security, sustainability, and the empowerment of local communities shapes its values and drives its operations. The company’s deep-rooted commitment to ethical practices and its ambition to be a leader in Sri Lanka’s food and retail sectors have enabled it to maintain long-standing trust with its consumers.

In this assignment, five of Cargills critical information assets, along with their potential weaknesses and vulnerabilities, have been carefully analyzed. These assets are fundamental to the company’s operational efficiency and are integral to sustaining its supply chain and customer satisfaction.

The five critical assets are
1. Supply Chain Management System
2. Retail Point-of-Sale (POS) System
3. Payroll & Protected Data
4. Supplier and Contract Management System
5. Employee Payroll and Sensitive Data

We will complete "Allegro Worksheet 10" by identifying plausible threats for each scenario. The subsequent steps involve predicting the "probability level" for each threat based on sound justification, assigning appropriate "impact" values for each scenario, and proposing at least one risk mitigation strategy for each identify.

Allegro Worksheets & Justifications

ASSET 01: Supply Chain Management System

Worksheet 08

	Critical Information Asset Profile	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Supply Chain Management System	This system is important for keeping track of stock and working with suppliers for all its supermarkets and stores.	The system handles buying products, keeping track of stock, and making sure items are delivered, so that all supermarkets have enough supplies and everything is sent out smoothly.
(4) Owner(s) *Who owns this information asset?*		
IT Infrastructure and Operations Division		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Only authorized personnel in the supply chain management team can view sensitive inventory and procurement data.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Only authorized personnel in the supply chain management team can modify and update the inventory and procurement data. This asset must be available for authorized personnel to access, modify, and save the updated data as needed.
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The system must be available to all supermarkets and distribution teams to ensure continuous stock management and delivery.

	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	This asset must be available for 24 hours, 7 days/week, 52 weeks/year.
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	All users who have access to the system must authenticate themselves using multi-factor authentication to ensure secure access.

(6) Most Important Security Requirement
What is the most important security requirement for this information asset?

❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Worksheet 10

Risk Scenario 1: Insiders intentionally or accidentally leaking sensitive data to unauthorized external parties.

		Information Asset Risk Worksheet	
Information Asset Risk	**Threat**	Information Asset	Supply Chain Management System
		Area of Concern	Insiders intentionally or accidentally leaking sensitive data to unauthorized external parties.
		(1) Actor *Who would exploit the area of concern or threat?*	Disgruntled employee with system access
		(2) Means *How would the actor do it? What would they do?*	Misuse of system access to alter or delete supply chain data.
		(3) Motive *What is the actor's reason for doing it?*	deliberate
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**

		(5) Security Requirements *How would the information asset's security requirements be breached?*	When an insider alters or manipulates data, the accuracy and trustworthiness of the system's information are compromised. This can lead to incorrect decision-making and a lack of confidence in the system. Deleting data or disrupting system operations can affect the system's availability, causing downtime or delays in processing critical supply chain activities.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Disruption of the supply chain could lead to financial losses due to order delays, lost sales, and potential penalties.	Reputation & Customer	8	4
	Financial	7	3.5
The supply chain system being down or disrupted would hinder the company's ability to operate efficiently, causing productivity	Productivity	5	2.5
	Disruption of Services	7	3.5
This scenario is unlikely to directly affect safety or health, unless the system manages perishable goods that could spoil.	Fines & Legal Penalties	6	3
	Supply Chain Reliability	8	4
Relative Risk Score			**17.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Supply Chain Management Database	Administrative- • Implement a strict data classification policy. • Perform regular audits of user access to sensitive data. Techinical- • Apply encryption for data at rest and in transit.

	• Ensure regular backups. Physical- • Limit physical access to database servers by using biometric or card access controls. Residual Risk- • Some risk remains due to potential insider negligence or sophisticated attacks, but encryption and audits minimize it.
Employee Devices (Laptops, Tablets)	Administrative- • Enforce policies for regular security updates and patching. • Implement device usage guidelines, including remote work rules. Techinical- • Install endpoint protection (anti-virus, firewalls). • Enable remote wipe and encryption features for lost devices. Physical- • Restrict physical access to work devices using secure lockers or storage. • Use device locks. .Residual Risk- • Residual risk exists if employees fail to follow guidelines or lose devices, though encryption reduces unauthorized access.
Email Communication System	Administrative- • Enforce email usage policies, including secure email protocols. • Train employees on phishing and social engineering attacks. Techinical- • Deploy email encryption (PGP, S/MIME) for sensitive data. • Implement spam filters and phishing detection mechanisms. Physical- • Ensure email servers are physically secure and restricted to authorized personnel. Residual Risk- • Some risk from sophisticated phishing attacks may remain, but user training and encryption reduce overall vulnerability.
File Storage and Sharing Systems	Administrative- • Restrict access to file shares based on role. • Conduct regular audits of shared files and user permissions Techinical- • Use encrypted file storage. Apply Data Loss Prevention (DLP) tools to monitor and prevent unauthorized data sharing. Physical- • Secure file storage devices in locked rooms. • Use secure document shredding for printed copies Residual Risk- • Some residual risk from user error or malicious insiders remains, but encryption and DLP tools reduce exposure.

Third-Party Vendor Systems	Administrative- • Establish vendor security requirements and SLAs. • Require regular security assessments of vendors. Techinical- • Ensure secure API integrations. • Monitor third-party access to internal systems. Physical- • Restrict physical access to third-party vendors when on-site Residual Risk- • Residual risk from third-party breaches may remain, but careful monitoring and security contracts reduce overall impact.
Network Infrastructure (Routers, etc.)	Administrative- • Document network security policies and ensure all network changes are approved and logged. Techinical- • Use firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). • Implement VPN for remote access. Physical- • Restrict access to network infrastructure using biometric locks. • Ensure network rooms are physically secured. Residual Risk- • Minimal risk remains due to possible insider misuse, but strong network monitoring and controls greatly reduce this.

Justification of probability and Severity values of Risk Scenario 1

Attribute	Value	Justification
Probability	50%	The probability of an insider threat is moderate, considering that employees or other insiders with legitimate access might misuse their privileges. While access controls and monitoring are generally in place, the risk remains due to the potential for malicious intent or accidental misuse.
Reputation & customer confidence	8	An insider breach can severely damage trust, as customers expect internal data handling to be secure. It indicates a failure of internal controls and can cause a significant loss of confidence.

Financial	7	Financial impacts include losses from data manipulation, unauthorized transactions, and potential compensatory actions. Insider threats can cause direct financial harm but may be less extensive than widespread external attacks.
Productivity	5	While insider actions can disrupt operations, especially if data is altered or deleted, the impact is often less extensive than a full system compromise from an external attack.
Disruption of Services	6	Insider threats can disrupt services if the insider misuses access to alter, delete, or manipulate critical system data. Although the impact may not be as widespread as an external attack, services could be temporarily disrupted while the organization identifies and resolves the issue. The downtime can affect operations, order processing, or supply chain functionality. However, internal access can often be quickly revoked, minimizing long-term service interruptions, though the potential for serious damage remains.
Fines & Legal Penalties	6	Legal penalties for insider breaches depend on the severity and the data involved. Moderate severity reflects potential fines and legal consequences, particularly if sensitive customer data is compromised. Legal penalties for insider breaches depend on the severity and the data involved. Moderate severity reflects potential fines and legal consequences, particularly if sensitive customer data is compromised.
Supply Chain Reliability	**8**	Insider threats directly impact supply chain reliability, causing data inaccuracies and potentially disrupting operations. This high impact reflects the critical nature of internal data integrity.

Worksheet 10

Risk Scenario 2: Unauthorized individuals gaining access to sensitive data through an external cyberattack.

		Information Asset Risk Worksheet			
Information Asset Risk	**Threat**	Information Asset	Supply Chain management System		
		Area of Concern	Unauthorized individuals gaining access to sensitive data through an external cyberattack.		
		(1) Actor *Who would exploit the area of concern or threat?*	External hacker or a group of cybercriminals.		
		(2) Means *How would the actor do it? What would they do?*	A hacker might target weaknesses in the supply chain system, including outdated software lacking security patches, inadequate password policies, or phishing schemes to gain unauthorized access. After breaching the system, they could either extract sensitive data or create chaos by corrupting information or temporarily shutting down operations.		
		(3) Motive *What is the actor's reason for doing it?*	deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	The primary security requirements at risk are confidentiality and availability. Confidentiality would be breached if a hacker gains access to sensitive information, leading to unauthorized disclosure. Availability could be compromised if a cyberattack disrupts or shuts down the system, affecting the operational continuity of the supply chain management system.		
		(6) Probability	❑ **High**	❑ **Medium**	❑ **Low**

		What is the likelihood that this threat scenario could occur?			
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value**	**Score**
	Leaking sensitive data or experiencing system downtime can significantly damage a company's trust and reputation. Customers expect secure and reliable service, and when this trust is breached, it takes considerable time and effort to rebuild. A damaged reputation can lead to negative publicity and diminished customer confidence.		Reputation & Customer Confidence	6	3
			Financial	8	4
	Financial losses are often an immediate consequence of data leaks or system failures. These losses can arise from compensations to affected customers, lost sales, and increased costs to restore systems. Over time, the financial burden can escalate, especially if the breach deters new clients or drives existing customers away. In some cases, especially when perishable goods are involved, a breach or downtime can directly impact the delivery of products or services. This disruption may lead to missed deadlines, spoiled goods, and unmet customer expectations, all of which contribute to broader operational challenges.		Productivity	7	3.5
			Disruption of Services	6	3
	Data breaches often come with legal implications. Organizations may face fines and penalties from regulatory bodies for failing to protect sensitive information. Legal proceedings can be lengthy and costly, further adding to the financial and reputational damage. Compliance with data protection regulations becomes critical to avoid such outcomes. A breach of trust not only damages a company's reputation but also affects its ability to retain customers. Customers		Fines & Legal Penalties	5	2.5
			Customer Retention	5	2.5

	may choose to leave if they feel their data is at risk or if service reliability is compromised. Restoring confidence and retaining customers after a data leak or system downtime often requires significant investment in customer relations and enhanced security measures.			
	Relative Risk Score			**18.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Application Level	**Administrative Controls:** Regular software updates, secure coding practices, and application security training. **Technical Controls:** Application firewalls and input validation. **Residual Risk:** Unknown vulnerabilities (zero day attacks).		
Data Storage	**Administrative Controls:** Access control policies and regular audits. **Technical Controls:** Encrypt data at rest, database activity monitoring, and regular backups. **Residual Risk:** Potential insider threats and physical theft.		
Network Infrastructure	**Administrative Controls:** Network security policies and incident response planning. **Technical Controls:** Network segmentation, VPNs for secure access, intrusion detection systems (IDS). **Residual Risk:** Potential advanced persistent threats (APTs)		
Physical Environment	**Administrative Controls:** Implement access control lists for physical access. **Physical Controls:** Secure server rooms, surveillance cameras, and environmental controls (e.g., fire suppression). **Residual Risk:** Natural disasters and power failures.		
User Access Points	**Administrative Controls:** User training on phishing and social engineering. **Technical Controls:** Multi-factor authentication (MFA), endpoint protection software. **Residual Risk:** Phishing attacks that might bypass user awareness.		

-

Justification of probability and Severity values of Risk Scenario 2

Attribute	Value	Justification
Probability	50%	The likelihood of an external cyberattack exploiting vulnerabilities in the supply chain management system is moderately high. While many organizations implement security measures like encryption, firewalls, and MFA, the threat landscape constantly evolves. New vulnerabilities and sophisticated attack methods pose an ongoing risk, particularly if security measures are not regularly updated.
Reputation & customer confidence	6	A successful external attack resulting in unauthorized data access can significantly harm the company's reputation and customer trust. The severity is substantial but can be managed through prompt incident response, transparency, and efforts to reassure customers.
Financial	8	Financial losses from such a breach could be considerable, including costs for incident response, compensating affected parties, and potential loss of business. This risk is rated high due to the direct and indirect costs associated with such breaches.
Productivity	7	An external attack disrupting the supply chain management system could significantly impair operational productivity. Resource allocation to counteract the breach and system downtimes can cause a marked reduction in operational efficiency.
Disruption of Services	7	An unauthorized external access attack targeting the supply chain management system could lead to significant disruption of services. The system may need to be taken offline to prevent further exploitation, investigate the breach, and apply necessary security patches. During this time, the interruption could hinder the normal operation of supply chain activities, causing delays in service delivery, order processing, and overall business operations. While services will eventually be restored, the disruption could be considerable depending on the extent of the attack.

Fines & Legal Penalties	5	Legal penalties could arise if the breach violates data protection laws. The extent depends on regulations and the nature of the data involved, with moderate severity reflecting potential fines and legal repercussions.
Customer Retention	**5**	A successful external cyberattack can lead to unauthorized access to sensitive customer information or operational disruptions. If customers perceive the company as unable to protect their data or maintain consistent service, they may choose to take their business elsewhere. However, if the breach is managed effectively and customer concerns are promptly addressed, the impact on customer retention can be somewhat mitigated. Therefore, this impact is considered moderate, reflecting the balance between potential customer loss and the opportunity to retain them through effective communication and resolution efforts.

-

ASSET 02: Payroll & Protected Data

Worksheet 08

All Allegro - Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset ***What is the critical information asset?***	**(2) Rationale for Selection** ***Why is this information asset important to the organization?***	**(3) Description** ***What is the agreed-upon description of this information asset?***
Payroll & Protected Data	**This system handles the processing of employee salaries and manages sensitive personal data.**	**The Employee Payroll and Sensitive Data system manages payroll data, including salaries, bonuses, deductions, tax information, and personal employee details, ensuring accurate salary payments.**
(4) Owner(s) ***Who owns this information asset?***		
HR and Finance Department		
(5) Security Requirements ***What are the security requirements f***	***or this information asset?***	
❑Confidentiality	**Only authorized personnel can view this information asset, as follows:**	**Protection of sensitive employee data such as salary details, bank information, and personal details to prevent unauthorized access and ensure privacy.**
❑ Integrity	**Only authorized personnel can modify this information asset, as follows:**	**The accuracy of payroll data is vital for ensuring that employees receive the correct salaries and benefits.**

❑Availability	**This asset must be available for these personnel to do their jobs, as follows:**	**The system needs to be reliably accessible for processing payroll and managing employee data at scheduled times to ensure timely salary payments.**
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	**The system must be available for 12 hours/day, 7 days/week, 52 weeks/year, ensuring that payroll processing can occur without interruptions.**
❑Authentication	**This asset has special regulatory compliance protection requirements, as follows**	**All users who have access to the payroll system must authenticate themselves using multi-factor authentication (MFA) to comply with regulatory protection requirements. This ensures that only authorized individuals can access sensitive payroll information.**

(6) Most Important Security Requirement			
What is the most important security requirement for this information asset?			
❑ **Confidentiality**	❑ **Integrity**	❑ **Availability**	❑ **Other**

-

Worksheet 10

Risk Scenario 3: Theft or interception of sensitive employee payroll information, leading to identity theft, financial fraud, and legal consequences.

		Information Asset Risk Worksheet			
Information Asset Risk		**Information Asset**	Payroll & Protected Data		
		Area of Concern	Theft or interception of sensitive employee payroll information, leading to identity theft, financial fraud, and legal consequences.		
	Threat	**(1) Actor** ***Who would exploit the area of concern or threat?***	External hackers, insiders		
		(2) Means ***How would the actor do it? What would they do?***	Exploiting system vulnerabilities or using internal access to steal sensitive payroll data.		
		(3) Motive ***What is the actor's reason for doing it?***	deliberate		
		(4) Outcome ***What would be the resulting effect on the information asset?***	❑ Disclosure ❑ Destruction ❑ Modification ❑ Interruption		
		(5) Security Requirements ***How would the information asset's security requirements be breached?***	Sensitive employee information, such as salary details, personal identification, and bank account numbers, must remain private and protected from unauthorized access.		
		(6) Probability ***What is the likelihood that this threat scenario could occur?***	**❑ High** **75%**	**❑ Medium** **50%**	**❑ Low** **25%**
	(7) Consequences			**(8) Severity**	

	What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?	*How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	Unauthorized access or data manipulation can lead to fraud, incorrect salary payments, or the need to compensate employees for breaches, resulting in significant financial damage to the organization	**Reputation & Customer**	**8**	**4**
		Financial	**7**	**3.5**
	Breaches of sensitive payroll data can erode employee trust and damage the company's reputation, both internally and with the public, harming Cargills' overall image.	**Productivity**	**5**	**2.5**
		Disruption of services	**6**	**3**
	Failure to comply with data protection regulations can result in fines or legal action, particularly if confidential employee data is exposed or misused.	**Fines & Legal**	**6**	**3**
		Data loss	**8**	**4**
Relative Risk Score				**20**

(9) Risk Mitigation ***Based on the total score for this risk, what action will you take?***			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***		
Physical Controls	Restrict access to the physical locations (e.g., server rooms) where payroll systems and databases are housed. Use biometric access or keycards.		
Physical Controls	Ensure that workstations used by HR and finance staff are secured, with automatic screen locks and monitoring of USB ports to prevent unauthorized data transfers.		

-

Technical Controls	Use encryption for data at rest and in transit to protect sensitive payroll data
Technical Controls	Enforce MFA for access to payroll systems, reducing the likelihood of unauthorized access even if login credentials are compromised.
Administrative Controls	Implement role-based access control (RBAC), ensuring only authorized personnel (HR, finance, IT) can access payroll data. Review and update access permissions regularly.

Justification of probability and Severity values of Risk Scenario 3

Attribute	Value	Justification
Probability	**50%**	The likelihood of sensitive payroll information being stolen or intercepted is moderate. While robust security measures like encryption and access controls are in place, vulnerabilities such as phishing attacks or insider threats could still exploit gaps. Therefore, the risk is neither too high nor too low.
Reputation & customer confidence	**8**	The impact on reputation and employee confidence is high if sensitive payroll data is stolen. Employees trust the organization to protect their personal and financial information, and any breach could severely damage that trust. Employees may feel insecure about the safety of their data, leading to potential employee dissatisfaction, reduced morale, and a negative perception of the company in the wider public.
Financial	**7**	The financial impact could be substantial, including costs related to investigation, compensation for affected employees, legal fees, and potential loss from fraudulent transactions. While it could strain the financial resources of the organization, having a strong incident response plan and insurance could mitigate the losses to some extent, keeping the financial risk moderate.

Productivity	**5**	The theft of payroll information would affect productivity as resources will need to be diverted toward investigating the breach, fixing vulnerabilities, and managing employee concerns. While the effect on overall business operations may not be extreme, there will be notable distractions and delays, especially in the HR and IT departments.
Disruption of Services	**6**	The disruption caused by this type of breach could delay key processes such as payroll distribution, leading to employee dissatisfaction and operational slowdowns. However, the primary business operations are likely to remain unaffected in the long term, making this disruption moderate but significant during the incident.
Fines & Legal Penalties	**6**	Legal penalties could arise from non-compliance with data protection regulations (e.g., GDPR, CCPA), especially if employee data is exposed and misused. However, if the breach is reported promptly and appropriate remediation is carried out, the fines and penalties may be reduced. Nevertheless, this still represents a moderate financial and legal risk.
Data Loss	**8**	The loss of sensitive payroll data can have a severe impact, especially if the data is unrecoverable or manipulated. It can lead to payroll inaccuracies, identity theft, and other financial frauds. The integrity and confidentiality of employee data are paramount, and any loss could have long-lasting repercussions on both the employees and the organization.

-

Worksheet 10

Risk Scenario 4: Unauthorized Access & Data Manipulation

		Information Asset Risk Worksheet			
Information Asset Risk		**Information Asset**	**Payroll & Protected Data**		
		Area of Concern	Unauthorized Access & Data Manipulation		
	Threat	**(1) Actor** ***Who would exploit the area of concern or threat?***	Insider, External attackers		
		(2) Means ***How would the actor do it? What would they do?***	unauthorized access and data manipulation occur through system vulnerabilities, stolen credentials or phishing, and malicious insiders, leading to compromised payroll data, financial loss, legal issues, and damaged trust.		
		(3) Motive ***What is the actor's reason for doing it?***	Deliberate		
		(4) Outcome ***What would be the resulting effect on the information asset?***	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
		(5) Security Requirements ***How would the information asset's security requirements be breached?***	Confidentiality, due to unauthorized access to sensitive payroll data, and Integrity, because of the manipulation or alteration of payroll data, which undermines its accuracy and trustworthiness.		
		(6) Probability ***What is the likelihood that this threat scenario could occur?***	❑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**
	(7) Consequences ***What are the consequences to the organization or the information asset owner***			**(8) Severity** ***How severe are these consequences to the***	

	as a result of the outcome and breach of security requirements?	***organization or asset owner by impact area?***		
		Impact Area	**Value**	**Score**
	Expenses incurred from fraud or theft, including the costs of breach remediation, legal fees, and compensation for affected employees, which can significantly impact the company's financial stability.	**Reputation & Customer**	**7**	**3.5**
		Financial	**6**	**3**
	Decline in employee morale and trust due to the breach, leading to potential decreased productivity, increased turnover, and a strained workplace environment.	**Productivity**	**5**	**2.5**
		Disruption of services	**6**	**3**
	Potential fines and legal actions resulting from non-compliance with data protection regulations, which can include regulatory penalties and lawsuits from affected parties**.**	**Fines & Legal**	**5**	**2.5**
		Data loss	**7**	**3.5**
Relative Risk Score				**18**

(9) Risk Mitigation ***Based on the total score for this risk, what action will you take?***			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***		
Administrative Controls	Restrict access to payroll data based on user roles and responsibilities.		
Technical Controls	Use strong encryption for data at rest and in transit.		

-

Technical Controls	Implement MFA for accessing payroll systems.
Physical Controls	Restrict physical access to servers and data storage areas.

Justification of probability and Severity values of Risk Scenario 4

Attribute	Value	Justification
Probability	**50%**	The likelihood of unauthorized access and data manipulation is moderate due to potential vulnerabilities in security systems, including weak access controls, phishing, or insider threats. Security measures are likely in place, but evolving cyber threats and social engineering tactics keep the risk at a medium level.
Reputation & customer confidence	**7**	If unauthorized access and data manipulation occur, it could significantly impact customer confidence. Customers expect organizations to maintain data security and integrity, and any breach could damage trust. The impact on reputation would be notable, especially if sensitive customer data is compromised or misused.
Financial	**6**	Financial losses from unauthorized access could include the costs of investigating and resolving the breach, recovering lost or manipulated data, and compensating affected customers. Although substantial, financial losses would likely be contained through proper cybersecurity insurance or quick remediation, keeping the financial impact moderate.
Productivity	**5**	The incident would cause a temporary dip in productivity, as resources would need to be allocated to handling the breach. IT staff, legal teams, and other departments would be diverted from their usual tasks to mitigate the issue. However, once the issue is resolved,

		normal operations could resume fairly quickly, resulting in a moderate effect on productivity.
Disruption of Services	**6**	The disruption to services would be significant but manageable. Unauthorized access could interrupt business processes, prevent transactions, or cause delays in delivering services. However, if an effective incident response is in place, the service downtime would be minimized, keeping the disruption impact at a moderate level.
Fines & Legal Penalties	**5**	Legal penalties may arise due to non-compliance with data protection regulations, especially if customer or sensitive data is compromised. However, if the breach is swiftly detected, reported, and mitigated, the fines may be lower, resulting in a moderate legal risk.
Data Integrity	**7**	Data manipulation or loss could have severe consequences for the integrity of business operations. While backups and recovery mechanisms may reduce the risk of permanent data loss, the temporary manipulation or corruption of data could cause serious operational challenges. The severity is high, especially if critical data is altered.

ASSET 03: Retail Point-of-Sale (POS) System

Worksheet 08

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Retail Point-of-Sale (POS) System	This system processes customer transactions and is essential for the operation of all Cargills outlets.	The POS system handles customer purchases, processes payments, and tracks sales data across Cargills' retail stores.
(4) Owner(s) *Who owns this information asset?*		
IT and Retail Departments		
(5) Security Requirements *What are the security requirements f*	*or this information asset?*	
❑**Confidentiality**	Only authorized personnel can view this information asset, as follows:	Customer payment information must be accessed only by authorized staff to ensure sensitive financial data remains protected.
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Sales data must be accurately recorded and protected from unauthorized alterations to avoid financial discrepancies and ensure accurate reporting.
❑**Availability**	This asset must be available for these personnel to do their jobs, as follows:	The POS system must be operational during business hours across all retail locations to process transactions without interruption.
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	This asset must be available for *12* hours/day, *7* days/week, *52* weeks/year.

❑**Authentication**	. This asset has special regulatory compliance protection requirements, as follows	All users who have access to the Retail Point-of-Sale (POS) System must authenticate themselves using multi-factor authentication

(6) Most Important Security Requirement			
What is the most important security requirement for this information asset?			
❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Worksheet 10

Risk Scenario 5: Unauthorized personnel gain access to the POS system or compromise the system through external attacks (e.g., malware, hacking).

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	Information Asset	Retail Point-of-Sale (POS) System	
	Area of Concern	Unauthorized personnel gain access to the POS system or compromise the system through external attacks (e.g., malware, hacking).	
	(1) Actor *Who would exploit the area of concern or threat?*	Hackers, Cybercriminals	
	(2) Means *How would the actor do it? What would they do?*	Attackers exploit weak or default passwords, use phishing attacks to steal login credentials, and install malware or ransomware through malicious email attachments or compromised websites. Additionally, weak network security may allow unauthorized remote access to the POS system.	
	(3) Motive *What is the actor's reason for doing it?*	deliberate	
	(4) Outcome *What would be the resulting effect on the information asset?*	**❑ Disclosure**	**❑ Destruction** **❑ Interruption**
		❑ Modification	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality is breached when unauthorized access to sensitive data occurs. Integrity is compromised if transaction data is altered, causing discrepancies. Availability is affected when system	

			downtime prevents transactions from being processed.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	**Value**	**Score**
	Tampered sales records can lead to inaccurate financial data and cause financial losses. Additionally, stolen customer data may lead to fraud and a loss of revenue.		Reputation & Customer Confidence	6	3
			Financial	5	2.5
	Breaking laws or regulations can result in expensive fines and legal costs. At the same time, damage to the business's reputation can lead to a loss of customer trust, reduced sales, and challenges in attracting new clients. Both issues can have lasting impacts on the business's success and financial health.		Productivity	4	2
	If sensitive customer data, like payment information, is stolen, the business could face fines and penalties for violating data protection laws. This can lead to both legal and financial consequences.		Disruption of services	6	3
			Fines & Legal Penalties	4	2
			Data loss	5	2.5
				Relative Risk Score	**15**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical	Implement network firewalls and intrusion detection systems to monitor and prevent unauthorized access.		

Technical	Regularly update and patch software and hardware to fix vulnerabilities
Physical	Secure server rooms and network equipment with access controls and surveillance.
Physical	Restrict physical access to POS terminals and network infrastructure.

Justification of probability and Severity values of Risk Scenario 5

Attribute	Value	Justification
Probability	50%	The likelihood of unauthorized personnel gaining access to the POS system is moderate due to vulnerabilities like weak passwords, unpatched software, or phishing attacks. While security measures such as firewalls and intrusion detection systems are in place, attackers often find new methods to bypass protections, making the risk neither too high nor too low.
Reputation & customer confidence	6	Unauthorized access to the POS system can lead to some loss of customer trust, especially if payment or personal data is exposed. However, if the business reacts promptly, the impact may be somewhat mitigated, with moderate damage to reputation.
Financial	5	The financial impact includes the cost of recovering from the attack, addressing fraudulent transactions, and handling potential fines. While significant, the financial losses can be contained with proper incident response plans.

Productivity	4	Downtime caused by the attack will temporarily lower productivity, especially during the busiest times. However, the disruption is expected to be short-term, and operations can resume quickly once the issue is resolved.
Disruption of Services	6	The attack can disrupt services, prevent transactions from being processed, and cause delays, especially during peak times. The disruption, while significant, will be manageable with quick action to restore service.
Fines & Legal Penalties	4	If the attack leads to a breach of data protection laws, the business may face legal penalties. However, if the breach is detected and managed swiftly, the fines and penalties will likely be moderate.
Data Loss	5	While transaction data may be lost or manipulated, backups and recovery mechanisms can help minimize the overall impact. The damage is moderate but not devastating.

Worksheet 10

Risk Scenario 6: Customer payment data being stolen or intercepted during transaction

<table>
<tr><td colspan="3">Allegro - Worksheet 10</td><td colspan="4">INFORMATION ASSET RISK WORKSHEET</td></tr>
<tr><td rowspan="9">Information Asset Risk</td><td rowspan="9">Threat</td><td>Information Asset</td><td colspan="4">Retail Point-of-Sale (POS) System</td></tr>
<tr><td>Area of Concern</td><td colspan="4">Customer payment data being stolen or intercepted during transactions</td></tr>
<tr><td colspan="2">(1) Actor
Who would exploit the area of concern or threat?</td><td colspan="4">External attackers, Insiders</td></tr>
<tr><td colspan="2">(2) Means
How would the actor do it? What would they do?</td><td colspan="4">Malware or spyware can capture payment details during transactions, while man-in-the-middle attacks intercept data transmitted over insecure networks. POS terminal skimming devices can secretly collect card details, and exploiting unpatched vulnerabilities in POS software or systems can lead to unauthorized access and data breaches.</td></tr>
<tr><td colspan="2">(3) Motive
What is the actor's reason for doing it?</td><td colspan="4">deliberate</td></tr>
<tr><td colspan="2">(4) Outcome
What would be the resulting effect on the information asset?</td><td colspan="4">❑ Disclosure ❑ Destruction
❑ Modification ❑ Interruption</td></tr>
<tr><td colspan="2">(5) Security Requirements
How would the information asset's security requirements be breached?</td><td colspan="4">Stolen payment data, such as credit card information, can result in fraudulent transactions, leading to financial losses. This breach can erode customer trust and potentially result in legal action against the business. Additionally, failure to protect sensitive data may lead to regulatory fines and further financial penalties.</td></tr>
<tr><td colspan="2">(6) Probability
What is the likelihood that this threat scenario could occur?</td><td>❑ High
75%</td><td>❑ Medium
50%</td><td colspan="2">❑ Low
25%</td></tr>
<tr><td colspan="3">(7) Consequences
What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</td><td colspan="3">(8) Severity
How severe are these consequences to the organization or asset owner by impact area?</td></tr>
<tr><td colspan="3" rowspan="2">Payment data breaches can seriously harm a business's reputation and cause customers to lose trust. When trust is</td><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td>Reputation & Customer Confidence</td><td>7</td><td>3.5</td></tr>
</table>

	broken, it's hard to win back, making it difficult to retain customers and slowing down future business growth.	Financial	6	3
	Stolen payment data can result in financial losses from fraudulent transactions, and businesses may face substantial fines for failing to adhere to data protection regulations. These financial losses can put pressure on the company's resources and reduce profitability.	Productivity	4	2
	Customers affected by the data breach may pursue legal action to seek compensation for their losses. This could result in expensive legal disputes, increasing financial pressure on the company, and causing further harm to its reputation.	Disruption of services	5	2.5
		Fines & Legal Penalties	5	2.5
		Data loss	6	3
			Relative Risk Score	**16.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical	Implement network monitoring and intrusion detection systems to identify and respond to suspicious activities in real-time.		
Technical	Encrypt payment data both at rest and in transit to protect it from unauthorized access during transmission.		
Physical	Secure physical access to POS terminals and servers with surveillance, locks, and access controls. Install CCTV in the server room to prevent unauthorized entry.		

Justification of probability and Severity values of Risk Scenario 6

Attribute	Value	Justification
Probability	50%	The risk of customer payment data being stolen is moderate. Payment systems are a common target for cybercriminals, but many businesses have strong encryption, authentication protocols, and other security measures in place. However, the ever-evolving nature of cyber threats makes this risk a persistent concern.
Reputation & customer confidence	7	Theft of customer payment data can damage the company's reputation, causing customers to lose trust in its ability to secure sensitive information. The impact on reputation is significant but can be mitigated through timely communication and resolution efforts.
Financial	6	Financial losses could result from both fraudulent transactions and compensating affected customers. Additionally, the company may face revenue losses due to customer attrition. However, these losses are likely to be moderate if mitigated promptly.
Productivity	4	The breach may lead to operational disruptions as resources are diverted to investigating and addressing the issue. While this will slow down normal operations, the disruption is expected to be temporary.
Disruption of Services	5	If customer payment data is compromised, services may be temporarily halted to investigate the breach, implement fixes, and prevent further issues. While disruptive, this impact is likely to be short-term.
Fines & Legal Penalties	5	The company could face fines and penalties if the breach violates data protection regulations. However, the extent of these legal consequences will depend on the jurisdiction and the severity of the breach.

Data Loss	6	Payment data is highly sensitive, and its loss can have far-reaching consequences for both the business and its customers. However, the impact can be contained if proper backups and response mechanisms are in place.

References

[1]“Household,” Cargillsonline.com, 2020. https://cargillsonline.com/Product/Household?IC=MTA=&NC=SG91c2Vob2xk (accessed Sep. 19, 2024).

[2]“Cargills Food City Supply Chain,” SlideShare, Jun. 06, 2016. https://www.slideshare.net/slideshow/cargills-food-city-supply-chain/62770835

[3]“Cargills Ceylon,” YouTube. https://www.youtube.com/channel/UCUZtWongqwoNUjYSX7oUw-g (accessed Sep. 19, 2024).

[4]“Cargills Online - YouTube,” www.youtube.com. https://www.youtube.com/channel/UCJalrbJo6XQRGahj_iRMNAg (accessed Apr. 28, 2024).

[5]OpenAi, “ChatGPT,” chatgpt.com, 2024. https://chatgpt.com